



**Secured2** Beyond Encryption

# How Secured2 Uses Beyond Encryption Security to Protect Your Data

## Secured2 Beyond Encryption Whitepaper

Document Date: 06.21.2017  
Document Classification: Public  
Website Location: [www.secured2.com](http://www.secured2.com)  
Document Feedback: [info@secured2.com](mailto:info@secured2.com)

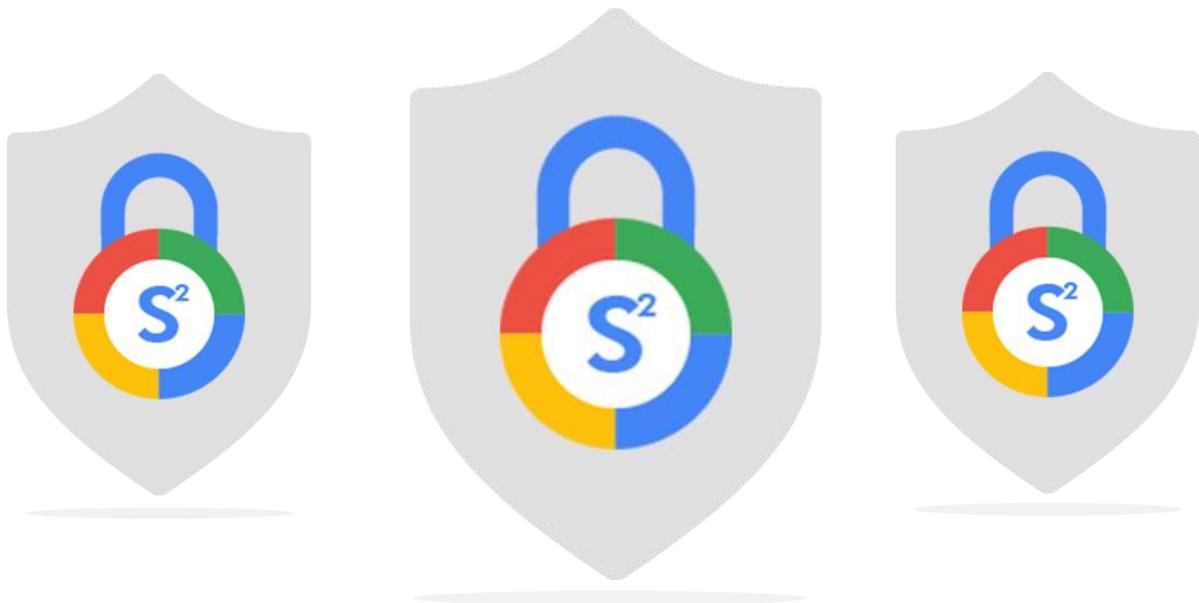
SECURED<sup>2</sup> is a Minnesota-based technology company founded with the mission of securing customer data and developing cutting-edge solutions that prevent data theft.

## Table of Contents

Introduction.....	3
How Secured2 Views Data Security.....	4
A new approach to data at rest.....	5
Data on Disks	
Key management and the decryption process	
Secured2's key management solution	
Auditing and Access Control	
Identity Management	
Data from backup media	
Protection of Data in Transit.....	9
Data traveling over the Internet	
Between you and Secured	
Conclusion.....	12

## Introduction

Here at Secured2, we understand that security is important for any organization that uses any kind of software application. Whether it's sending an email, to sharing a document with a colleague. Security needs to be a part of everything you use.



The core of our security strategy leverages our patented **Shrink > Shred > Secure > Restore** solution that fits into today's existing security solutions for over the wire, and at-rest encryption. The result is a security solution that keeps your data protected and away from hackers.

# How Secured2 Views Data Security

Today's encryption solutions work by replacing data with unreadable code known as ciphertext. Decrypting the ciphertext back into its original form, you need a key that is used on the algorithm to unlock the data. Attackers that want to go around or break encryption will first try stealing the keys (the easiest path) or try to find flaws in the encryption algorithms and their implementation. The strength of encryption is based on several different factors that include key length, key complexity and randomness of the key generation.

What we have learned with encryption is given enough time and computer power any form of encryption today can be broken. It's not a matter of if, but when you will get hacked. That's why encryption has gone from DES encryption to Triple DES, then AES 128-bit, to AES 256-bit and now larger key standards like Blowfish 448-bit encryption. As the computing power increases with Moore's Law so does the length of encryption keys to offset computing advancements. To date there are no 'mathematical proofs' that encryption even secures your data.

With the quantum computing world upon us the days of encryption (as the gold standard) to protect your data is over. We need new solutions that go beyond encryption to protect data and provide quantum resiliency. Secured2's team of world-class security engineers have pioneered exciting security technology that fits into today's security standards like SSL encryption, FDE AES Encryption and other means of encryption. So we can meet current standards while providing new layers of protection that finally offer 'proofs' data is secure.

Secured2 is the first security that is quantum resilient and also the first security that provides a cyber warranty to indemnify you against a data breach. Something no other security provider can or is providing.

---

We have learned with encryption given enough time and computer power any form of encryption can be broken.

# A new approach to Data Stored at Rest

At Secured2 we believe all your data stored at rest in your on-premise environment or in the cloud should be 100% under your control. Also, secured beyond the reach of hackers. That's why secured2 requires you to shred n' spread your data into 3 or more separated locations (multi-cloud, hybrid or local VM's). For more information on how we protect, replicate and scrambled data, please see the (Secured2 Infographic.) Secured2 also utilizes the best of breed cloud storage disaster recovery and business continuity solutions to ensure recovery from any catastrophic error or natural disaster at one of our partners data centers.

Data stored at rest is processed using the **shrink > shred > secure > restore** patented methodology of Secured2 with the added benefit of using existing security methods like encryption and key management. So we exceed all known data security standards.

## Data on Disks

A function of our security is to shred binary data into small segments, randomize the data segments and encrypt each segment using AES 256 bit encryption. We utilizes this security method for ALL of our products. This security happens without any intervention from the customer or having to take action. Making the security user friendly, integrated and tied to the user physically. Because to initiate the unlocking of data you need to verify identity through any number of available authentication / verification options.

---

Secured2 uses shrink, shred, secure, restore process to protect your data beyond encryption.

Each segment is encrypted and the key associated with each segment is 100% controlled by the customer. This means that nobody but the authorized customer can access data. As well, we use a dual key solution so if you ever forget or lose your key there is still a way to retrieve and access your data.

# How we manage keys and decrypt data

Managing keys safely and reliably, while giving you access, and control is central to authorizing services and the individuals using those services. Secured2 has built a robust and patented solution for distribution, generation, rotation and management of cryptographic keys using our proprietary security mechanism. In this section we will outline how we allow you to control your keys and prevent others from accessing your critical information from the 'spoofing' of your keys or compromising the encryption method.

## Secured2's key management solution

Managing keys safely and reliably, while giving you access, and control is central to keeping your data protected. Files and data from customer generated content is run through our proprietary process that breaks data into small 10k segments, randomizes the segments and each segment is given a layer of AES 256 encryption, then encapsulated in TLS encryption over the wire and is spread randomly into multiple storage location a customer chooses (multi-cloud, hybrid, local VM's or any storage variation they choose.)

*The result is an end-to-end security solution that protects data beyond encryption.*

Hackers can't steal your data because they can't find your data. Only you have the map and instructions to recover and reassemble data.

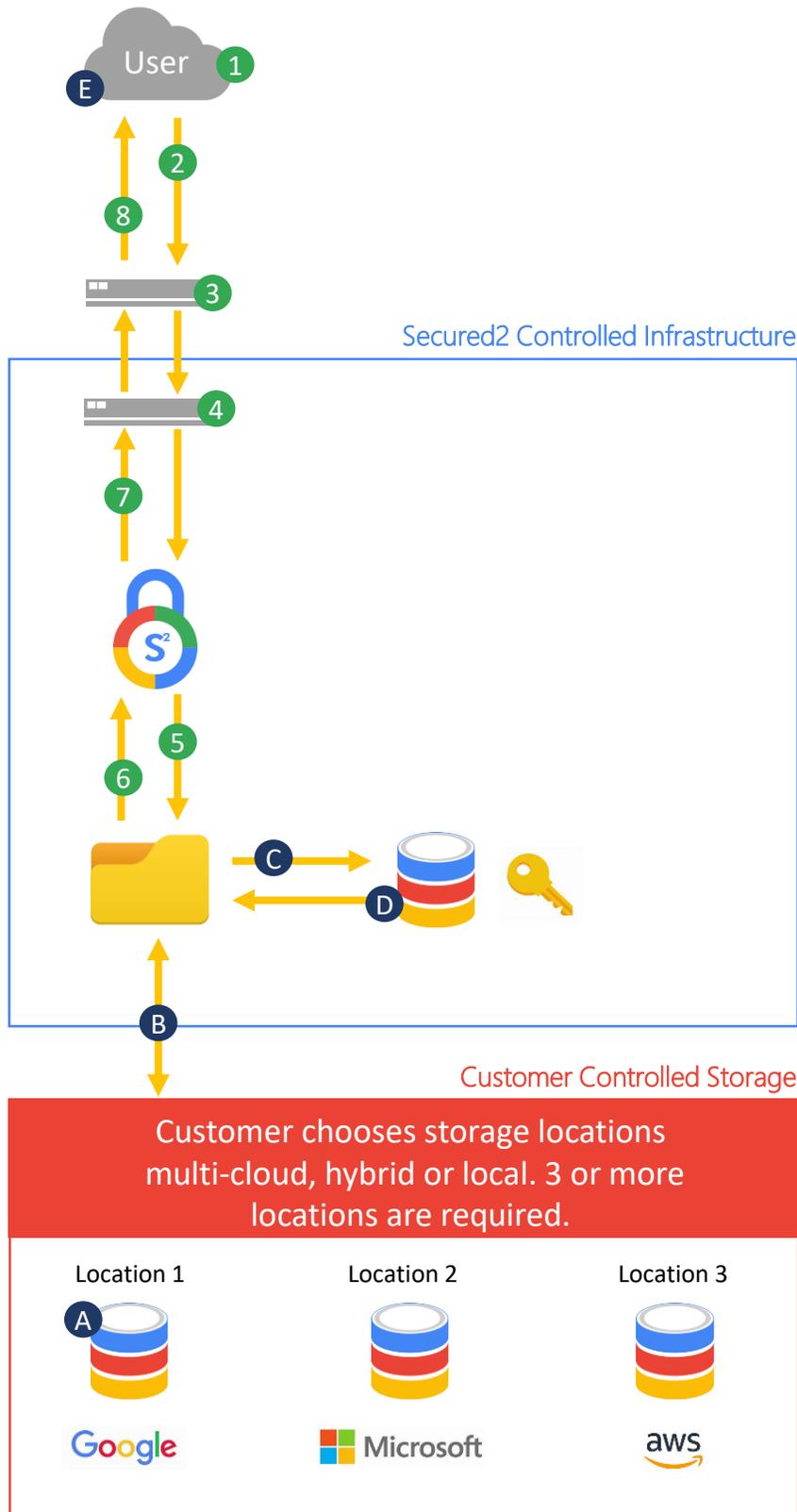
All access to data is tied to a person's physical identity using some form of identification or verification system. The customer can choose from out of the box offerings like (Google Auth, Windows Hello or RSA) or a customer can choose any vendor they like, and we can integrate the authentication for them. We believe a key way to ensure security is to ensure identity on the front-end. Best of all, a customer can control the locks on the front door using any authentication or verification vendor they choose & trust.



---

Secured2 customers can control the locks on the front door using any authentication or verification vendor they choose & trust.

# Security flow diagram



## Step by step process

- 1 Initiate Request**  
User authenticates to Secured2 and requests drive data.
- 2 Encrypted Tunnel**  
SSL/TLS-based encryption dependent on users browser
- 3 Secured2 Front End**  
Directs traffic to AFEs
- 4 Application Front End / Cloud Mover**  
Directs traffic to app servers
- 5 Requests User Data**  
User's request goes from the application to storage
- 6 Fetch Data**  
Grab encrypted data segments
- 7 Stage Data & Key Approval**  
Secured2 holds assembly keys and customer holds unlock keys (dual key system)
- 8 Decrypt & Assemble Data**  
SSL/TLS-based encryption for sending back data, customer unlocks using their private keys.

## Data Restoration

- A Data Retrieval**  
Data segments are fetched from multi-cloud storage of a customers choice
- B Key Check**  
Is the requester authorized to access the data
- C Verification / Authentication**  
The request is verified and if authorized returns the request for data access.
- D Send Protected Data**  
Directs traffic to app servers
- E Decrypt Data**  
Storage System decrypts data and user can access the information.

## Auditing and Controls

Secured2 has designed our solution to prevent the access of Secured2 employees or any third party from accessing your data. The only person that can access or decrypt any data is the 'authorized' party who originally created the data. The Secured2 process has been independently verified, scrutinized and audited to ensure that no customer information is ever 'at risk' through any form of unauthorized breach. Only the people and applications that have been 'approved' through verification can be granted access. Secured2 does have access to log data that allows us to ensure our systems are operating in a secure manner and following our strict guidelines.

---

Through a function of our security process nobody from Secured2 at any point can touch, change, access or alter your data. Secured2 only knows your data location but has no way to unlock the data.

Through a function of our security process nobody from Secured2 at any point can touch, change, access or alter your data. Secured2 only knows your data location but has no way to unlock the data.

### [Data on backup media](#)

Secured2 also utilizes the full-disk encryption provided by all cloud partner companies to even further protect your data at rest. So you get the benefits of the Secured2 shrink, shred, secure, restore technology in addition to all the cloud-based security offered by our partners Microsoft, Google and Amazon.

We are in continual communication with our partners and convey any changes to their security stance such as updates, enhancements and improvements. However, we do not rely on the security of our partners because data run through our process is secured beyond encryption. Think of the security provided by cloud partners as just another layer of complexity.

# Protection of Data in Transit

As we've shown, Secured2 protects customer data at rest on both disks and backed up into the cloud. But we also protect your data while it's being delivered from one place to another. Ensuring anything being transmitted is protected beyond encryption.

## Data being sent over the Internet

When you use any Secured2 solution, your information travels between your browser, Secured2's cloud mover and the ultimate end storage destinations you choose such as Google, Microsoft or Amazon. In these situations, encryption has long been used to protect your data. Unfortunately, today's it's simply not enough to encrypt data. With Secured2, we add new levels of protection that live in concert with existing solutions like TLS.

All data being sent across the internet is first run through our algorithmic process that shrink, shreds and secures data. During this process, your data is randomized, broken into small segments and randomly distributed into the multiple storage locations you choose. The fact all data is 'processed' before going over the Internet ensures that each packet being sent is completely random, not in sequential order (like today's encryption) and done as a function of our solution. Guaranteeing if any packet is intercepted via packet sniffing that a hacker gets nothing of any value if they are able to subvert normal encryption techniques. This ensures your data security and prevents outside intruders from accessing your data.

## Protecting you from Secured2 & Cloud providers

Today when you use the cloud most cloud vendors hold the keys and have total access to your data. When you use Secured2 *you are in total control of the security.*

We have purposely built our solution, so you are in total control of security. We cannot see or access your data because you control the keys that reverse our security process. So all your data is under your control.

How this works is by using a two-key system. The first key you control and is tied to whatever verification system you use (facial recognition or multi-factor) and the second key we manage that knows where your data lives. So if you ever lose your key, we know where the data lives so you can unlock.

---

The fact all data is 'processed' before going over the Internet ensures that each packet being sent is completely random, not in sequential order (like today's encryption) and done as a function of our solution.

## Conclusion

The Secured2 patented **Shrink > Shred > Secure > Restore** process allows you the security and fluid access to your data by utilizing our data masking and data shredding technology.

**SHRINK >** Until now, data compression technology hasn't changed much since the 1990s. The SECURED<sup>2</sup> patented **transmogrification** process converts and compresses your data into a secure state that reduces the data footprint up to 80%.

**SHRED >** We digitally "shred" your data into fully randomized segments that are impossible for anyone or anything to comprehend. The SECURED<sup>2</sup> customized shredding process verifies that your data can be stored anywhere without the fear of it being hacked, scanned, or stolen.

**SECURE >** As SECURED<sup>2</sup> is storage agnostic, you can now store your shredded data at any cloud host or storage server of your choice. Acting like a RAID controller, it must have a minimum of three hosts, but can be expanded to hundreds of providers.

**RESTORE >** Seamlessly use your data just like it's all on your hard drive. Whether it's a document, photo, or database – retinal, facial, or multi-factor authentication will make sure you are the only person accessing your data on any endpoint.

### Your Experience

We believe that each customer is entitled to data protection and unparalleled customer service. First, we'll send out our team to advise you on how best to implement your Secured2 data security solution. Second, we help implement with our highly certified team of experts. Then you can expect your SECURED<sup>2</sup> everyday experience will be fluid, user friendly, and really no different than how you work today.

### Beyond Encryption & Quantum Resilient Technology

When we say unhackable, we mean unhackable. This isn't coming from the marketing department; this claim is from third party FBI, CIA, DOD trained experts. Secured2 compresses, converts, and secures your data in a proprietary process which is simply secure! It's the first non-binary security ever created.

---

We believe that each customer is entitled to data protection and unparalleled customer service.

#### **Don't believe us? The CIA, FBI, and DoD agree.**

Click [here](#) for Security Report

"In vitro analysis of the encoded data set showed no revealing patterns or indications of information leakage." - Allied Security Analysis

#### **SECURED<sup>2</sup> Helps protect you from:**

- Hackers
- WAN/LAN Data Packet Sniffing
- Backdoor Access
- Marketing Information Scanning
- Compliance Violations